Amendments to the Claims

This listing of claims supersedes all prior listing of claims.

1.   (Currently Amended) A method of providing authentication services for applications that are running on a client and requiring access to a network based server, the method comprising:

establishing a network connection further comprising an authentication with the network;

generating, responsive to the authentication, a <u>first</u> dynamic seed locally at the ~~client and the~~ network based server;

<u>generating, responsive to the authentication, a second dynamic seed locally at the client without utilizing the first dynamic seed, wherein the generated second dynamic seed is consistent with the first dynamic seed;</u>

generating ~~an~~ <u>first</u> application key independently at the ~~client and the~~ network based server corresponding to the locally generated <u>first</u> dynamic seed; ~~and~~

<u>generating a second application key independently at the client corresponding to the locally generated second dynamic seed, wherein the second application key is generated without utilizing the first application key;</u>

providing the generated <u>first</u> application key to facilitate authenticating an <u>application at the network based server and the generated second application key to facilitate authenticating an application at the client.</u>

2.   (Currently Amended) The method of claim 1 wherein ~~the~~ generating ~~an~~ <u>the first</u> application key further comprises storing the <u>first</u> application key <u>at the network based server</u> for

subsequent retrieval to facilitate the authenticating an application <u>and wherein generating the second application key further comprises storing the second application key at the client for subsequent retrieval to facilitate the authenticating an application</u>.

3.   (Currently Amended) The method of claim 1 wherein ~~the~~ generating ~~an~~ <u>the first</u> application key further comprises generating a plurality of application keys where each of the plurality of keys corresponds to a different application <u>and wherein generating the second application key further comprises generating a plurality of application keys where each of the plurality of keys corresponds to a different application</u>.

4.   (Currently Amended) The method of claim 1 wherein ~~the~~ providing the <u>first</u> application key further comprises[[;]] providing an application seed and generating keying information specific to the application <u>and wherein providing the second application key further comprises providing an application seed and generating keying information specific to the application</u>.

5.   (Currently Amended) The method of claim 1 wherein ~~the~~ providing the <u>first</u> application key further comprises providing a new application key every time the authenticating the application is required <u>and wherein providing the second application key further comprises providing a new application key every time the authenticating the application is required</u>.

6.   (Currently Amended) The method of claim 1 wherein ~~the~~ providing the <u>first</u> application key further comprises providing the <u>first</u> application key corresponding to a time

duration within which the <u>first</u> application key is valid <u>and wherein providing the second</u> <u>application key further comprises providing the second application key corresponding to a time</u> <u>duration within which the second application key is valid</u>.

7.   (Currently Amended) The method of claim 1 wherein the ~~obtaining~~ <u>generating</u> the <u>first</u> dynamic seed further comprises ~~obtaining~~ <u>generating</u> a new dynamic seed each time an authentication with the network occurs, the generating the <u>first</u> application key further comprises generating a new application key corresponding to the new dynamic seed, and the providing the <u>first</u> application key further comprises providing the new application key.

8.   (Original) The method of claim 1 wherein the authentication with the network utilizes processes corresponding to an Extensible Authentication Protocol.

9.   (Original) The method of claim 1 implemented by one of a client and a network server.

10.   (Original) The method of claim 9 implemented by one of a wireless client and a network server accessed via a wireless network.

11.   (Currently Amended) A computer readable medium storing programming instructions for operating a system entity to provide authentication services for applications that are running on a client and requiring access to a network based server, including programming instructions for:

establishing a network connection and completing an authentication with the network, the authentication generating a <u>first</u> dynamic seed locally at ~~the client and~~ the network based server <u>and generating a second dynamic seed locally at the client, wherein the second dynamic seed is generated without utilizing the first dynamic seed</u>;

generating [[an]] <u>a first</u> application key independently at the ~~client and the~~ network based server based on the ~~locally generated~~ <u>first</u> dynamic seed <u>and a second application key independently at the client based on the second dynamic seed</u>; and

providing, on demand, the <u>first and second</u> application key<u>s</u> to facilitate authenticating an application.

12.   (Currently Amended) The computer readable medium of claim 11 wherein the programming instructions for storing the <u>first</u> application key in persistent storage <u>at the network based server and the second application key in persistent storage at the client</u> for subsequent retrieval to facilitate the authenticating an application.

13.   (Currently Amended) The computer readable medium of claim 11 wherein the programming instructions for generating a plurality of application keys where each of the plurality of keys is derived from the <u>first and second</u> dynamic seed<u>s</u> and corresponds to a different application.

14.   (Previously Amended) The computer readable medium of claim 11 wherein the programming instructions providing the application key further provides an application seed; and wherein the computer readable medium further comprises the programming instructions for using the application seed for generating keying information specific to the application.

15.   (Previously Amended) The computer readable medium of claim 11 wherein the programming instructions for providing a different application key every time the authenticating the application is required.

16.   (Currently Amended) The computer readable medium of claim 11 wherein the programming instructions for providing the <u>first and second</u> application key<u>s</u> and the <u>first and second</u> application key<u>s</u> further corresponds to a time duration within which the application key is valid.

17.   (Previously Amended) The computer readable medium of claim 11 wherein the programming instructions for providing a new dynamic seed each time an authentication with the network occurs, and for generating a new application key corresponding to the new dynamic seed and providing the new application key to facilitate the authenticating the application.

18.   (Previously Amended) The computer readable medium of claim 11 wherein the programming instructions for completing the authentication with the network utilizes processes corresponding to one of a smart card, an Extensible Authentication Protocol with Subscriber Identity Module extensions, an Extensible Authentication Protocol with Transport Level Security extensions, and an Extensible Authentication Protocol with Authentication and Key Agreement extensions.

19.   (Previously Amended) The computer readable medium of claim 11 implemented by one of a client and a network server.

20.   (Previously Amended) The computer readable medium of claim 19 implemented by one of a client operating within a wireless communication unit and a network server accessed via a wireless network.